

**Session # 4 Best
Practices:
People and
Procedures**



Content Notes

Presentation Notes

Have slide showing as attendees assemble.

Introduce yourself, giving a brief review of IS background and instructional experience.

NOTE: Be prepared to answer questions throughout the presentation. If attendees look as if they do not understand a given point, take time to explain.



Content Notes

Review 4 basic steps of Information Security Solutions:

- Analysis
- People
- Procedures
- Technology

Presentation Notes



Content Notes

This presentation will focus on

- Procedures
- People

Let's start with procedures

Presentation Notes

Transition: Explain that you will now focus on procedures, though, obviously, people and technology coexist with the procedures themselves...



Best Practices: Procedures

Start with:

- **Security Policy and**
- **Mission Statement.**



Page 4

Content Notes

Applying Policies to Your Company

Use your organization's Security Policy and Mission statement (analysis) for developing procedures to be used in various aspects of your business:

Presentation Notes



Best Practices: Procedures

Determine where you need procedures.

- IT Security Policies
- System Administration Guidelines
- Web-Hosting
- E-Commerce Guidelines

Page 5

Content Notes

- Where IT security procedures are needed
 - Windows NT/2000 Security Guidelines
 - Data Server Guidelines
 - Network Security Policy
 - Email security
- System administration guidelines
- Web-hosting and/or E-Commerce Guidelines

Presentation Notes

Explain that procedures will cover some or all of these areas.

Explain that secure business procedures includes using caution with telephone queries.



Best Practices: Procedures

Determine who will need procedures.

- All employees, who use computers in their work
- Help Desk/system administrators
- System maintenance
- IT Out-Sourcing
- Software Applications

Then follow your procedures!

Page 6

Content Notes

- Who needs IT security procedures
 - All employees, who use computers in their work
 - Help Desk/system administrators
 - System maintenance
 - IT Out-Sourcing: Criteria for dealing with vendors and contractors
 - IT Applications: Criteria for purchasing software

Presentation Notes

Explain that procedures will cover some or all of these types of employees.



Best Practices: Procedures

Enforcing safe

- Internet practices
- E-mail practices
- Desktop practices
- Personnel practices


Page 7

Content Notes

Procedures:

- How you and your employees use the Internet
- Email practices: what to do when receiving email from someone you do not know; what to do when you receive an attachment
- How to safeguard a password for your desktop computer

Presentation Notes



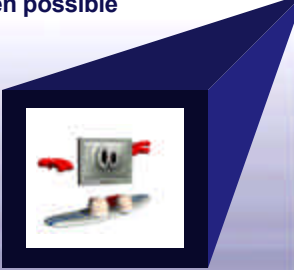
Safe Internet Practices

Do not:

- Download files from unknown sources
- Run files on web pages when possible

Do:

- Protect passwords, credit card numbers, and private information in web browsers



Page 8

Content Notes

Do not download any games, tools, documents, spreadsheets, or executable software

- Unless you know it is from a reputable and trusted source, and company policy will allow you to do so.
- Consider the running of JavaScript, code, or executables directly on the web page to be the same as downloading it (because it is)
- JavaScript: programs that are started when you browse to a page
- Examples of running code:
 - Opening a document to read it
 - Playing a sound file
 - Clicking on a “.exe” file link
- Do not ever submit any passwords, credit card numbers, or private information via web browser, unless a secure session is active (the “padlock” or the unbroken “key” is visible on the bottom)
- Assume that your web browsing is not private unless you’re assured that it is by a reputable site, and a secure session is active .

Presentation Notes

Explain the potential threats.

Ask how many have made credit card purchases on line. Ask how many of them have seen the padlock icon.

Safe Internet Practices (cont'd)

Do:

- **Configure your browser to “safe” or “Internet” security settings**



Page 9

Content Notes

Do not download any games, tools, documents, spreadsheets, or executable software

- Unless you know it is from a reputable and trusted source, and company policy will allow you to do so.
- Consider the running of JavaScript, code, or executables directly on the web page to be the same as downloading it (because it is)
- JavaScript: programs that are started when you browse to a page
- Examples of running code:
 - Opening a document to read it
 - Playing a sound file
 - Clicking on a “.exe” file link
- Do not ever submit any passwords, credit card numbers, or private information via web browser, unless a secure session is active (the “padlock” or the unbroken “key” is visible on the bottom)
- Assume that your web browsing is not private unless you’re assured that it is by a reputable site, and a secure session is active .

Presentation Notes

Explain the potential threats.

Ask how many have made credit card purchases on line. Ask how many of them have seen the padlock icon.

A presentation slide titled "Safe E-Mail Practices" with a blue and white striped graphic on the left. The slide lists three bullet points: "Be careful opening attachments", "Make sure your e-mail software is properly configured", and "Do not reply to all unsolicited emails". On the right side, there is a 3D blue cube with a white square in the center. The background is a light blue gradient. The text "Page 10" is in the bottom right corner.

Safe E-Mail Practices

- Be careful opening attachments
- Make sure your e-mail software is properly configured
- Do not reply to all unsolicited emails

Page 10

Content Notes

- Do not open any email attachments that are from strangers, or any unexpected or unexplained ones from people you know
 - Beware of the “passing on a great joke/game/tool” from a friend (they may not know they’re passing on a Trojan Horse)
 - Configure mail software to not preview or automatically open messages

Presentation Notes

Ask for ideas why it is a good idea to set for “do not preview.”

Safe Desktop Practices

Do:

- Use passwords
- Use computer accounts
- Use screen locking
- Log on and off



Page 11

Content Notes

Good Desktop Computer Security Practices

- Do not write down passwords
- Do not use the “Save Password” feature on login forms
- Do not share computer accounts
- Utilize account/screen locking (with password unlock)
 - If not available, then you should log off
- Logoff at the end of the day!
- Lock your laptop up when leaving the office

Presentation Notes

Ask how many have seen coworkers write down passwords so they won't forget them and then post the password near the computer.

Explain the rationale for each practice.

A presentation slide titled "Safe Personnel Practices" with a red underline. It features a list of four "Do:" items: confirm identities, accompany vendors, give only enough information, and properly dispose of sensitive information. The slide has a blue and white graphic on the left and a "Page 12" label at the bottom right.

Safe Personnel Practices

Do:

- Confirm identities of people and organizations
- Accompany all vendors, repair persons
- Give only enough information
- Properly dispose sensitive information

Page 12

Content Notes

Good Desktop Computer Security Practices

- Do not write down passwords
- Do not use the “Save Password” feature on login forms
- Do not share computer accounts
- Utilize account/screen locking (with password unlock)
 - If not available, then you should log off
- Logoff at the end of the day!
- Lock your laptop up when leaving the office

Presentation Notes

Ask how many have seen coworkers write down passwords so they won't forget them and then post the password near the computer.

Explain the rationale for each practice.



Implement Backup Procedures

Goal is ability to restore systems and data to what existed before any:

- **Virus incursions**
- **Theft or destruction**
- **Data integrity problems**

Page 13

Content Notes

The Value of Data Backups to Info. Security

Bad things will happen to your information

- Intentional, accidental, unknown, unplanned

A regular and verified backing up and preservation of all information is a cornerstone to Information Security

- Backup all files, software, and configuration data from all computers

Goal is to be able to restore systems and data to what existed before any:

- Virus incursions that destroyed data/systems
- Theft and destruction of information
- Intrusions that call to question system and data integrity
 - The “wipe clean and start over” fall-back

Keep an up to date inventory of all h/w and s/w over \$n.

Presentation Notes

Point out that these tips are important for home computer use, as well as office use.

Transition: So far, the topics covered have related to electronic security issues; now we'll discuss physical security issues.



Implement Physical Security

Facilities

- **Locks**
- **Anonymity**
- **Alarms**
- **Guards**
- **Floor-to-ceiling walls**



Page 14

Content Notes

Practice basic facility security

- **Locks** (doors, desks, file cabinets) Keep doors locked at all times to unattended rooms with computers and equipment (e.g. phone closets, communications gear)
 - Keys
 - Cipher locks
 - Access cards
- **CipherLocks or access cards** for frequent traffic into areas that house your important information
- **Anonymity** - Do not use signs such as "Server Room" on doors
- **Alarms**
- **Guards**
- **Floor-to-ceiling walls** around these sensitive areas

Presentation Notes

Explain the danger.

Explain the potential problems.



Implement Physical Security

Software/Hardware

- **Store securely**
- **Isolate sensitive data**
- **Monitor dial-in modems**
- **Physically separate computers**
- **Install removable hard drives**
- **Use tie-down cable locks**

Page 15

Content Notes

Secure Software:

- *Store securely* - Lock away all software disks, backup disks/tapes
- *Isolate sensitive data* - Consider isolating payroll, financial, or systems with very sensitive data from both the internal network and the internet
- *Monitor dial-in modems* - Beware of direct modem dial-in connections to a computer. Many have them, and they can answer calls made to them
- *Physically separate computers* - Physically separating computers can go a long way
- **Hardware (and Data) Theft Prevention Devices:**
 - Install Removable hard drives - locked away at night
 - Use tie-down cable locks for laptop and desktop systems

Presentation Notes

Explain the danger.

Explain the potential problems.



Implement Personnel Security

- **Conduct background checks.**
- **Control employee entrance and exit.**
- **Control employee departures.**



Page 16

Content Notes

Good Personnel and Procedural Security

Conduct background checks for employees, especially:

- Security personnel (including IT security)
- System administrators
- Persons who you trust with your most sensitive information

“Background checks” can be credit checks, criminal history, check of personal references

Have Employment entrance/exit security procedures

When an employee departs:

- Quickly deactivate all computer accounts
- Repossess keys, access cards, parking passes, etc.
- Change any door key codes or common passwords (yikes!) that employee knew about

Develop a checklist to use when employees exit the company.

Presentation Notes

Ask how many attendees work for companies that conduct background checks on any employees. Ask how many attendees do not know whether or not the company conducts background checks. Comment on their value.

Explain why common passwords are never advisable.

Transition: Passwords are an extremely important Information Security issue....



Implement Procedural Security

- Document keys holders.
- Protect company directories and contact information.
- Control passwords.



Page 17

Content Notes

Always document who has received keys, access cards, etc.

Protect Company directories and contact info

- They can make “social engineering” a lot easier for an outsider


Practice Help Desk Hygiene

- Verify all requests for password resets and privilege changes
- Call back the user to issue a new password

Presentation Notes

Explain why common passwords are never advisable.


Transition: Passwords are an extremely important Information Security issue....



Password Control

Make it difficult:

- To guess someone's password
- For password cracking tools to work
- To use compromised passwords



Page 18

Content Notes

Guidelines for Good Passwords

Goal is to make is difficult to:

- Guess someone's password
- Thwart password cracking tools which use dictionaries or brute force
- Continue damage with compromised passwords

Presentation Notes



Password Control (continued)

- **At least 8 characters long**
- **No names or birth dates**
- **At least one:**
 - Upper case
 - Lower case
 - Numeric
 - Special character
- **Change every 45-60 days.**

Page 19

Content Notes

Make all passwords at least 8 characters long

- Even longer is much better

Do not use only words, names, birth dates, etc.

Require at least one upper case, lower case, numeric, and special character

Change passwords every 45-60 days

- Do not allow recently used passwords to be reused

Presentation Notes

Give examples of good password guidelines: (require 8 digits, at least 1 number, at least one special case, etc...)

Ask for additional examples of good passwords (or pass phrases.)

Transition: Explain that there are resources for password creation and other procedures...



Password Control (continued)

- Limit reuse
- Pass phrases better than pass words

Bad Passwords

Password
Jimmy
NCC1701

Good Passwords

BeeBep#5
crk*Prf1
United We Stand 2day!

Page 20

Content Notes

- Do not allow recently used passwords to be reused
- Consider the use of pass phrases, rather than pass words.

Bad passwords:

- Password
- BeeBep#5
- jimmy

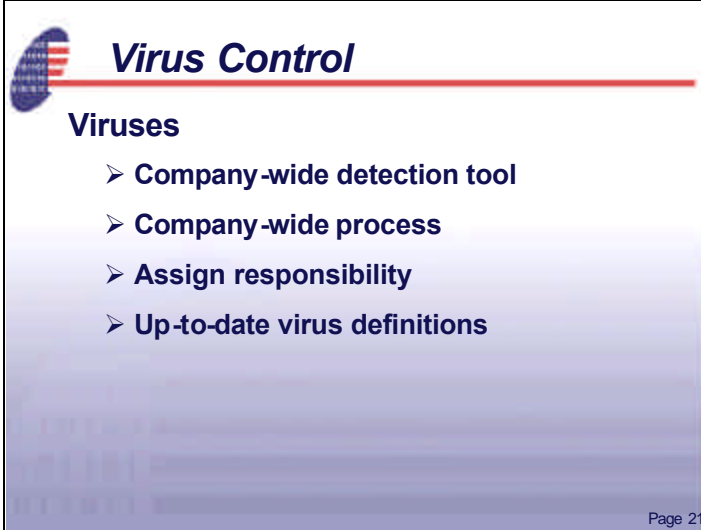
Good passwords:

- crk*Prf1
- NCC1701
- United We Stand 2day!

Presentation Notes

Ask for additional examples of good passwords (or pass phrases.)

Transition: Explain that there are resources for password creation and other procedures...

A presentation slide titled "Virus Control" with a red horizontal line. The slide has a blue and white graphic on the left. The background is a light blue gradient. The text "Virus Control" is in a large, bold, blue font. Below it, the word "Viruses" is in a smaller, bold, blue font. A bulleted list follows, with each item preceded by a blue right-pointing arrow. The list items are "Company-wide detection tool", "Company-wide process", "Assign responsibility", and "Up-to-date virus definitions". In the bottom right corner, it says "Page 21".

Virus Control

Viruses

- Company-wide detection tool
- Company-wide process
- Assign responsibility
- Up-to-date virus definitions

Page 21

Content Notes

Viruses

- Have a company-wide tool for detection of virus infections
- Have a process (and someone to oversee it) for reacting to virus infections
- Maintain up-to-date virus definitions in your tool!

Presentation Notes

Give examples of typical tools.

Explain how this should work.

Explain this responsibility.



Guidelines and Checklists

**Hardware and software vendors as a
resource**

**Other information
is on your resource
CD**



Page 22

Content Notes

Use Self-Assessment Guides and Checklists

You are not alone! – Computer Security Resources, Tools, and Associations are available to help you secure your enterprise.

NIST Security Guides and Bulletins

- Guides provide “how to” for managing security
- ITL Bulletins each fully cover a particular topic in computer security in easy to understand language
- Refer to vendors for system recommendations.

FBI InfraGuard Program

- Information on threats, vulnerabilities, and protections
- Local cooperative chapters for businesses, academia, law enforcement

NSA Security Checklists

- Configuration checklists for better securing Windows NT/2000, Routers, Servers, and other components

Small Business Administration - ProNet

- Information sharing and expertise contacts

Presentation Notes

Review the particular strengths of each resource.

Transition: As we review some of the most important procedures, we have to remember that maintenance and update are just as important as the initial implementation.



Systems Current & Patched

- **Possible vulnerabilities to:**
 - Operating Systems
 - Applications
 - Network
 - All other hardware and software

- **Updated patches and safeguards**



<http://icat.nist.gov/icat.cfm>

Page 23

Content Notes

Keep Your IT Systems Current and Patched!

Track and understand current and new vulnerabilities to Operating Systems, Applications, Network, and all other HW/SW that you have

- Consult vendor bulletins, ICAT

Deploy new patches and safeguards as they become available

- The hackers start looking for unpatched systems immediately

Presentation Notes

Explain ICAT

Give examples of titles



Systems Current & Patched

Consider security of potential products:

- How does vendor find/fix security problems?



Page 24

Content Notes

When selecting new or replacement IT systems or software, consider how secure the products are

- See how many vulnerabilities exist for the product on ICAT
- Ask how the vendor finds and fixes security problems
- Remember, their security problems will be your security problems

Presentation Notes

Give examples.



Content Notes

Presentation Notes

Explain that commitment to security is essential with all employees, at every level. However, the roles can be divided...

Ask for a few ideas on the role of management before going to the next slide.

Award prizes for responses and share ideas with the group.



People

**Management
commitment**

**Staff awareness
and
training**



Page 26

Content Notes

Presentation Notes

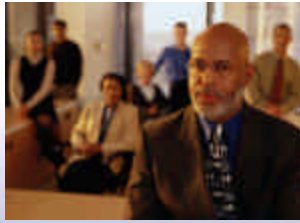
Explain that commitment to security is essential with all employees, at every level. However, the roles can be divided...

Ask for a few ideas on the role of management before going to the next slide.

Award prizes for responses and share ideas with the group.



Management: A Vital Role



- **Basic understanding of InfoSec best practices**
- **Ability to measure success**

Page 27

Content Notes

Management commitment: basis for all successful information security efforts.

Without that commitment it's unrealistic to think that the most aware employees or the most elaborate InfoSec procedures will protect your organization's data.

Presentation Notes



Management: A Vital Role

Includes:

- **Defining roles and responsibility**
- **Committing necessary resources**
- **Enforcing procedures**
- **Being involved**



Page 28

Content Notes

Presentation Notes

Explain bullets, focusing on:

- **Committing necessary resources**
- **Enforcing procedures**



Management: A Vital Role

To justify your organization's InfoSec plan:

- **Analyze your Information Security risks.**
- **Identify what needs to happen to secure the information you decide to protect.**



Page 29

Content Notes

Business Justification should be done in two ways:

- Analyze the Risk (loss) versus Protection (cost)
 - Find common ground with Business Risk Analysis
- Identify the Business Requirements/Enhancements being enabled by security

Without this, all else fails!

Presentation Notes

Explain the relationship

Transition: "Implementation necessitates total staff involvement."

Ask for ideas on how all employees are involved in IS.



Staff Awareness and Training

Begins with the first day at work:

- Security policies and procedures
- Security threats and cautions
- Basic security “do’s and don’ts”

Continues with reminders and tools:

- Pamphlets, posters, newsletters, videos
- Rewards for good security
- Periodic re-training

Page 30

Content Notes

Security Training and Awareness Tips

Ultimately, it's employees that secure your data.

Show employees on the first day of their employment:

- Company security policies and procedures
 - Ask for signed acknowledgement
- Security threats, cautions, and procedures
- Basic computer security “do’s and don’ts”

Continue with reminders and Tools:

- Pamphlets, posters
- Newsletter
- Videos
- Rewards for practicing good security
- Periodic re-Training

Presentation Notes

Explain that awareness and training are shared responsibilities

Explain that staff involvement is vital to implementation and success of the plan.

Explain how these incentives are helpful.

Explain the importance of training updates.



Training: Focus



- Why InfoSec is important to the organization
- What the organization's InfoSec policy is
- What InfoSec procedures the staff is expected to follow

Page 31

Content Notes

Training is necessary for establishing sound enterprise security and accountability

Conduct Security Training and Awareness

Should at least cover security reasons, policies, and procedures for secure business behavior

Presentation Notes

Explain that cooperation is always better when everyone is included in the “why” as well as the “what.”

Explain that in ideal circumstances, there is opportunity for staff to have input.



Key to Successful Training

Tailor training to your staff and the roles they play.



Page 32

Content Notes

Key is to tailor training towards the staff and their roles

Web-based or computer-based training methods are highly effective for IT staff

Presentation Notes

Give examples of other types of training and their appropriateness to varying groups:

- Instructor led
- One on one
- Job aids; electronic reminders, etc.



Staff Awareness and Training

**Take advantage of government
resources.**



Page 33

Content Notes

An Introduction to Computer Security: The NIST Handbook

Presentation Notes

Tell attendees that the handbook is on the CD.

Review contents and ways to use the handbook as a resource.



Content Notes

What do you do if the unthinkable happens?

Emphasize the importance of reporting breaches.

Know where to turn for Investigative and Forensic Support

- You may need specialized tracking, investigation, and evidence collection of malicious acts and computer crimes
- You may need support for personnel action, law enforcement (FBI, cybercrime divisions), and legal discovery process

Presentation Notes

Explain the resources.

Explain how to make this contact locally.



Content Notes

NOTE: Ask participants to take a few minutes to fill out the evaluation form for this presentation, which is at the end of the presentation handout. Put the filled out evaluation form on the table at the back of the room.

Presentation Notes

Transition: Explain that the next presentation will focus on technology.

If there is time, use the following questions:

What is your company's most valuable information? (Generally speaking. No secrets, please)
How long would your company survive if you lost that information or had it changed irreparably?
How valuable is that information to your competitor?

How vulnerable do you feel your systems are right now? Why?

- Best type of answer is "very", because "I don't know if they're not vulnerable" – and should get a prize

How you ever tested security?

Or was it "field tested" for you?

Can anyone tell us with certainty that the computer on their desk is patched with all the latest security updates as of last week?

- they get a prize if they can